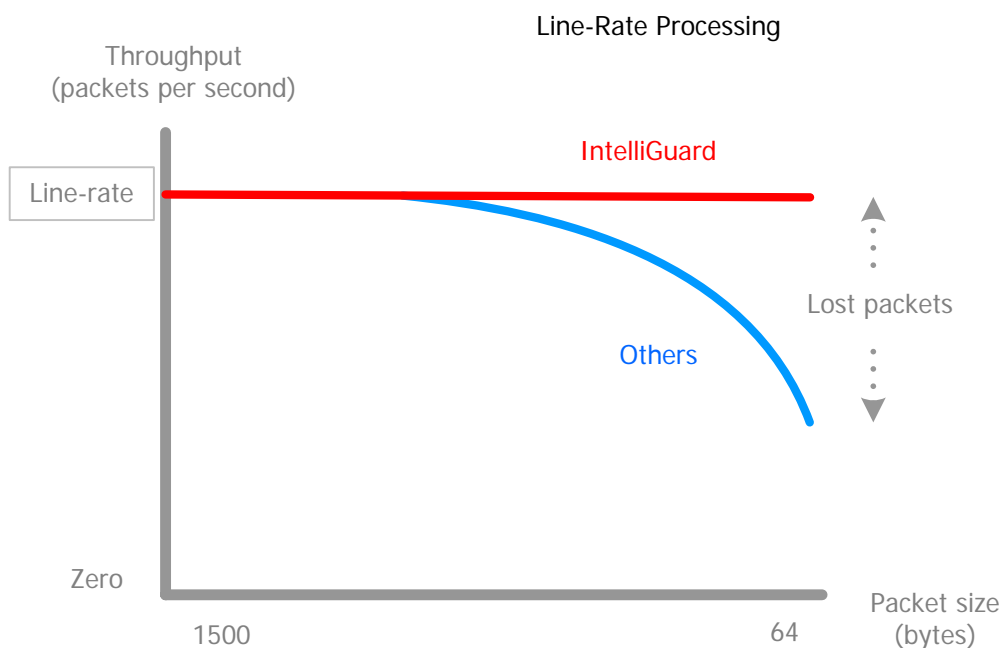


# Small Packet Attacks

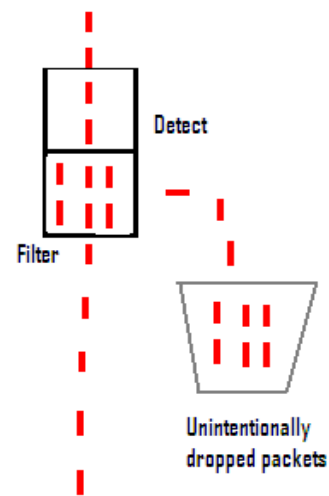
*Line-rate throughput is required under worst-case conditions*

Where a DDoS defence system is unable to process full line-rate, it will contribute to the DDoS attack by dropping legitimate packets. Attackers can generate any size packets they want, and simply bring about this failure situation by generating large numbers of small packets, thus making the DDoS defence system the weakest link in the network.

The only defense against small packet attacks is true line-rate performance.

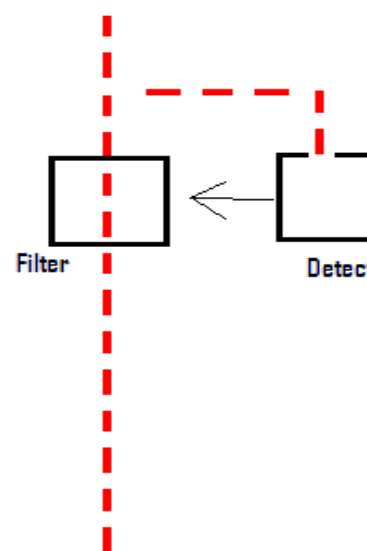


*Rival systems may provide line rate performance only under best case conditions, and thus fail to keep up with all packets on the wire with small packet sizes. IntelliGuard's DPS can process full line rate at 64 byte packets.*



**Rival Systems**  
– high latency

Filtering performed in primary traffic path, which causes bottlenecks that lead to unintentionally dropped packets and increased latency. This prevents their use in conjunction with services such as VoIP that suffer from latency and packet loss.



**IntelliGuard DPS**  
– low latency

Copies of packets are sent to detection system for analysis so that the filtering path remains clear. Performing all packet inspection off the primary traffic path enables true line-rate performance with negligible latency and zero packet loss.